METHOD FOR SECURE MULTICAST REPEATING ON THE PUBLIC INTERNET

INVENTOR
Ian A. Stewart

FIELD OF THE INVENTION

This invention relates to systems and methods for transmission of data on the Internet.

BACKGROUND OF THE INVENTION

A Multicast broadcast is an Internet broadcast with a "Class D" address. The devices that route information in the Internet (routers) recognize a Class D address as a Multicast and forward the Multicast data to requestors of the Multicast. The result is that Multicast saves Internet bandwidth by sharing the information as needed. Multicasting makes the multicast data available to a wide array of users. The wide dissemination over a public network also places the data at risk for interception by unauthorized recipients

Encryption was created for computers to move data in a secure fashion. Many different encryption formats have been used throughout the years. One problem however, is that encrypted data cannot be used by programs that do not possess the data key, and more importantly programs that do not posses the algorithm to de-crypt the data. An example of encryption at work is the Secure Sockets Layer of Transmission Control Protocol. This encryption scheme allows Internet browsers to exchange credit card information without being intercepted by hackers. The problem is that no Multicast programs support encrypted transmission. Therefore, there exists a need to allow the secure Multicast broadcasts.

SUMMARY OF THE INVENTION

The present invention comprises a system and method for sending a secure multicast transmission. The system includes a computer system coupled to a public network and configured to generate a multicast broadcast, and encrypt the generated multicast broadcast. The system also includes a router coupled to the public network, and a user system configured to request to join a multicast broadcast, wherein the user system is associated with the router. The router is configured to retrieve the encrypted multicast broadcast from the computer system over the public network, decrypt the sent multicast broadcast, and send the decrypted multicast broadcast to the user system requesting to join.

In accordance with further aspects of the invention, the computer system includes a router locally coupled to a multicast broadcast generating system. The multicast broadcast generating system attaches a local address to the generated multicast broadcast and sends the generated multicast broadcast with the local address to the router. The computer system router removes the local address, encrypts the sent multicast broadcast, and attaches a network multicast address to the encrypted multicast broadcast.

In accordance with other aspects of the invention, wherein a plurality of user systems are associated with the router.

As will be readily appreciated from the foregoing summary, the invention provides a technique for performing secure multicast transmissions.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred and alternative embodiments of the present invention are described in detail below with reference to the following drawings.

FIGURE 1 is a block system diagram of the present invention;

FIGURE 2A and B are flow diagrams performed by the system shown in FIGURE 1; and

FIGURES 3-8 illustrate examples of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in FIGURE 1 the present invention is a system 20 for performing secure transmission of multicast broadcasts. The system 20 includes a multicast private network 22, one or more multicast receiving private networks 24, and a public network 30. The private network 22 includes a multicast generating unit 36 coupled to a router 38. The router 38 is coupled to the public network 30. Each of the plurality of private networks 24 includes a router 42 that is coupled to the public network 30 and coupled to one or more user units 44. Examples of user units 44 are personal home computers, laptops, or any other computer processing device that allows wired or wireless connection to the public network 30 through the router 42 or Internet provider, such as AOL or AT&T.

The multicast private network's router 38 or some other computer device within the private network 22 receives a multicast broadcast from the multicast generating unit 36. An encryption application program executed on the multicast private network's router 38 or some other computer device within the private network 22 encrypts the received multicast broadcast for transmission to user units 44 that have requested the generated multicast broadcast. The router 42 of a receiving private network 24 retrieves the generated multicast encrypted broadcast, if a user unit 44 associated with the router 42 has requested to join the multicast broadcast. The retrieved multicast broadcast is decrypted by an application program executed on the router 42 or on some other computer device within the private network 24 and delivered to the requesting user unit 44. The method performed by the system 20 is described in more detail below in FIGURES 2A and 2B.

The present invention takes away the encryption and decryption steps from the end users and places that task to the nearest router. By performing the decryption at a router or Internet provider's server, associated with a large number of user systems, the encryption only needs to be performed once and not at every user system requesting to join the multicast broadcast.

As shown in FIGURE 2A, the process of performing secure multicast transmission over a public network 30 is shown. First, at decision block 100, the process determines if a user at a receiving server system or public network 24 desires to join a particular multicast broadcast. If no request to join a multicast broadcast exists the system thus continues until a request to join does occur. If a request to join a multicast broadcast has occurred, the multicast generating unit 36 generates and sends a multicast broadcast to the router 38 using a local address, see block 102. The local address used is known by the router 38 to be associated with a multicast broadcast. Next, at decision block 104, the router 38 determines if the address associated with the generated multicast broadcast indicates the need to perform encoding of the multicast broadcast information. If the router 38 does not detect a multicast address associated with the received data, the process returns to checking if the local address of a data packet received from a connected unit is associated with a particular multicast address. However, if the transmission (packet) received by the router 38 has a local address associated with a multicast broadcast requiring encryption, the router 38 encrypts the multicast data included in the received transmission (packet), see block 106. It can be appreciated that various types of data encryption can occur, for example, secure socket layer encryption or other types of the encryption can be used.

Next, at block 108, the original local address associated with the multicast broadcast sent to the router 38 is removed and a public multicast address is applied to the encrypted multicast data. Next, at block 112, as shown in FIGURE 2B, the encrypted

multicast data is transmitted to a receiving router 42 at a private network 24. The receiving router 42 is one which an associated user unit 44 has made a request to join a generated multicast broadcast. At block 114, the receiving router 42 decrypts the encrypted multicast data and, at block 116, the router 42 also removes the address associated with the received encrypted multicast data and applies a address local to the receiving private network 24. Finally, at block 118, the decrypted data is sent to the user unit 44 that requested to join the multicast broadcast according to the applied local address.

Example

The following refers to FIGURES 3-8. A data stream is first broadcast over on a private network on unicast private address 192.168.170.200 network address 192.168.170.1/24. See FIGURE 7. A transmission program is watching for address 192.168.170.200 and a gateway router has been programmed to not forward to private network 192.168.170.1/24. See FIGURE 5. When the packet/data stream on address 192.168.170.200 is spotted, it is placed into a buffer where the data portion of the packet is stripped. Then the data portion is encrypted and reaffixed to a Multicast packet header. The packet is then retransmitted on Multicast address 224.0.22.253. See FIGURE 7. The retransmitted information is routed to the public Internet, or broadcast on the airwaves, satellite, etc. See FIGURE 8. The system that receives the retransmitted information has private network 192.168.171.1/24. The gateway router on this private network is programmed to receive multicast groups. See FIGURE 4. The gateway router does not repeat a private Multicast Address 224.0.22.254 (note the address is different than the one specified above). The program at the receiving system requests a multicast join toward the rendezvous point at the source router. The rendezvous point is configured with the multicast address 224.0.22.254. A program on the receiving side is continuously joined to Secure Multicast 224.0.22.253 and the data is stripped away from the packet 224.0.22.253 decrypted and retransmitted on Multicast address 224.0.22.254 thus the Multicast Join is satisfied within the network and the requesting program sees it as any other Multicast. See FIGURE 6.

While the preferred embodiment of the invention has been illustrated and described, as noted above, many changes can be made without departing from the spirit and scope of the invention. Accordingly, the scope of the invention is not limited by the disclosure of the preferred embodiment.